Jméno: _____ Datum: _____ Body: _____

Recenze Proton VPN

Technická analýza ženevského Proton VPN, multihop směrování Secure Core, DNS filtry NetShield, audity open-source klientů a obfuskace protokolu Stealth.

PŘEHLED VÝUKY: RECENZE PROTON VPN

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede technickým přehledem Proton VPN. Prozkoumáte multihop směrování Secure Core, blokování DNS NetShield, audity open source klientů a obfuskaci protokolu Stealth.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte konfigurace VPN a zabezpečení sítě.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce nejlepšími VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/protonvpn/

Váš studijní plán: Proton VPN

- Analyzujte technickou architekturu a šifrovací standardy recenze Proton VPN.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte proprietární tunelovací protokoly se standardními implementacemi.

POKYNY K RECENZI PROTON VPN

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na uzly Secure Core a blokování NetShield. Zakončete bonusovou aktivitou Mysli rychle.

UZLY SECURE CORE A OPEN-SOURCE IMPLEMENTACE KLIENTŮ (ÚVOD)

Proton VPN je proslulý svým vícenásobným směrováním Secure Core a blokátorem obsahu NetShield DNS. Udržuje plně open source, nezávisle auditované klientské aplikace provozované pod jurisdikcí Ženevy ve Švýcarsku.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Jaká funkce Protonu směruje provoz přes bezpečné země?**

- A) Secure Core
- B) NetShield
- C) Tunel Stealth
- D) VPN Accelerator

2 **2. Jaká je hlavní funkce NetShield od Proton VPN?**

- A) Blokátor reklam a malwaru na úrovni DNS
- B) Šifrování datové části AES-256
- C) Dynamická rotace IP adres
- D) Obsluha přesměrování více portů

3 **3. Jaký protokol Protonu obchází DPI pomocí TLS handshaků?**

- A) Protokol Stealth
- B) WireGuard
- C) OpenVPN TCP
- D) L2TP/IPSec

4 **4. Co je jedinečné na zdrojovém kódu klientů Proton VPN?**

- A) Plně open-source a veřejně auditované
- B) Proprietární binární soubory s uzavřeným kódem
- C) Pronajaté ze šablon open-source repozitářů
- D) Uzavřený kód s vládními přístupovými portály

5 **5. Jak Proton VPN Accelerator optimalizuje rychlost?**

- A) Používá řízení zahlcení BBR a více jader CPU
- B) Automaticky přepíná na nešifrované HTTP
- C) Směruje provoz přes veřejné webové proxy
- D) Vypíná pravidla firewallu klienta

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Technologie Secure Core od Proton VPN směruje provoz uživatelů nejprve přes hardwarově zabezpečené fyzické servery umístěné v neutrálních, vysoce zabezpečených jurisdikcích.

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. NetShield funguje tak, že zachytává a blokuje požadavky na připojení k doménám trackerů a malwaru ve fázi dotazu DNS.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Zdrojové kódy klientů Proton VPN jsou drženy přísně proprietární, aby se zabránilo odhalení bezpečnostních zranitelností.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Protokol Stealth balí VPN pakety do standardního šifrování TLS, takže jsou k nerozeznání od HTTPS provozu.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Proton VPN působí pod panamskými zákony a spadá pod zpravodajské dohody 14 očí.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. K obejití pokročilých DPI firewallů mohou uživatelé v nastavení klienta zapnout vlastní protokol _____ .

2. Klientské aplikace Proton VPN vznikají jako _____ , takže je mohou auditovat externí výzkumníci.

3. Dynamický DNS blokátor filtrující škodlivé domény se nazývá _____ .

4. K obraně proti korelačním útokům na úrovni sítě směřuje provoz přes serverové uzly _____ .

5. Odchozí latenci a ztrátu paketů zmírňuje proprietární VPN _____ .

6. Právní sídlo Proton AG je v Ženevě a metadata účtů tak chrání _____ .

ZÁSOBNÍK SLOV

AKCELERÁTOR | KILL SWITCH | NETSHIELD | OPEN SOURCE | SECURE CORE | STEALTH | ŠVÝCARSKO | WIREGUARD

Sem napište své odpovědi:

1.
2.
3.
4.
5.
6.

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

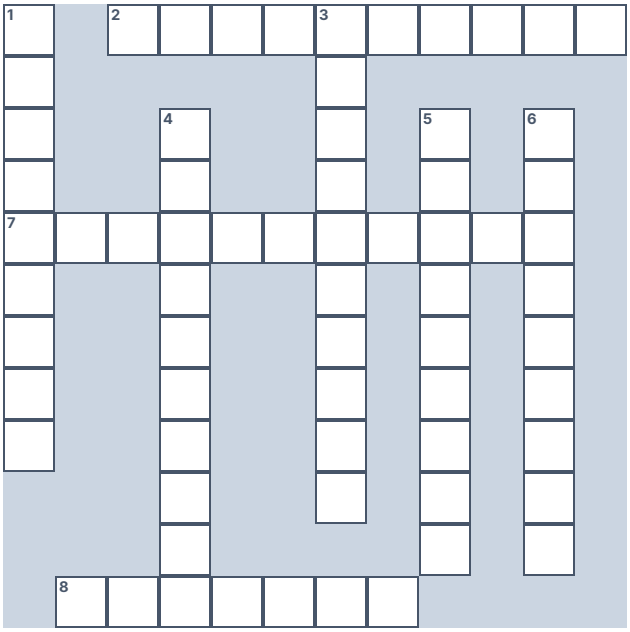
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. Secure Core	A	Moderní vysokorychlostní open-source protokol pro připojení.
☐	2. NetShield	B	Veřejně čitelný repozitář zdrojového kódu aplikace.
☐	3. Stealth	C	Motor optimalizace výkonu rozdělující zátěž procesoru.
☐	4. Akcelerátor	D	Blokátor reklam, trackerů a malwaru na bázi DNS.
☐	5. Open source	E	Centrální jurisdikce ochrany soukromí se sídlem ve Švýcarsku.
☐	6. Švýcarsko	F	Vlastní obfuskovaný protokol navržený k obcházení DPI filtrů.
☐	7. WireGuard	G	Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích.
☐	8. Kill Switch	H	Směrování multihop přes vysoce zabezpečené serverové uzly.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

2. Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10)

7. Optimalizační výkonnostní engine rozdělující zátěž procesoru (11)

8. Vlastní obfuskovaný protokol navržený k obcházení DPI filtrů (7)

SVISLÉ NÁPOVĚDY

1. Ústřední jurisdikce ochrany soukromí se sídlem ve Švýcarsku (9)

3. Vícenásobné směrování přes vysoce zabezpečené serverové uzly (10)

4. Veřejně čitelný repozitář zdrojového kódu aplikace (10)

5. Blokátor reklam, sledovačů a malwaru na úrovni DNS (9)

6. Moderní vysokorychlostní open-source protokol připojení (9)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

2 vodorovně: Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10 písmen):

7 vodorovně: Optimalizační výkonnostní engine rozdělující zátěž procesoru (11 písmen):

8 vodorovně: Vlastní obfuskovaný protokol navržený k obcházení DPI filtrů (7 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Ústřední jurisdikce ochrany soukromí se sídlem ve Švýcarsku (9 písmen):

3 svisle: Vícenásobné směrování přes vysoce zabezpečené serverové uzly (10 písmen):

4 svisle: Veřejně čitelný repozitář zdrojového kódu aplikace (10 písmen):

5 svisle: Blokátor reklam, sledovačů a malwaru na úrovni DNS (9 písmen):

6 svisle: Moderní vysokorychlostní open-source protokol připojení (9 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

C D Ž V Ě K G N Ž D Ň Ď Ř X Q

C R Ú B A Ž O E D L Š A Ď Ó Ď

E A É G I D S T Ř N V E I Š Ž

C U T É Ř Ů E S A Á Ý Ř P O Q

R G U Y R A J H S U C Š Č K Ň

U E Ý B Ě K Š I X W A Í A I S

O R Ž Ý Ý C L E F I R N S L J

S I N M Ť E P L G R S Ř G L Ž

N W Á Ó Ů L Ě D Ú C K Ý H S Š

E Ý B G M E Ž F J Ó O Q T W O

P S E C U R E C O R E X L I C

O N Ž Z Ě Á Ý P W Ú L Ů A T Q

B Ó V Ť N T F Ů Č Ý Ú K E C S

Á X Ž Y N O Š R X H P D T H Á

Č J Ř V W R X L Í H U H S Ě B

SEZNAM SLOV

SECURECORE NETSHIELD STEALTH AKCELERÁTOR OPENSOURCE

ŠVÝCARSKO WIREGUARD KILLSWITCH

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY
A. SECURECORE
B. NETSHIELD
C. STEALTH
D. AKCELERÁTOR
E. OPENSOURCE
F. ŠVÝCARSKO
G. WIREGUARD
H. KILLSWITCH

DEFINICE A POLE K PŘIŘAZENÍ
1. Optimalizační výkonnostní engine rozdělující zátěž procesoru.
2. Veřejně čitelný repozitář zdrojového kódu aplikace.
3. Moderní vysokorychlostní open-source protokol připojení.
4. Ústřední jurisdikce ochrany soukromí se sídlem ve Švýcarsku.
5. Vlastní obfuskovaný protokol navržený k obcházení DPI filtrů.
6. Blokátor reklam, sledovačů a malwaru na úrovni DNS.
7. Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích.
8. Vícenásobné směrování přes vysoce zabezpečené serverové uzly.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny virtuální privátní sítě (VPN). Odpovědi pište do připravených polí.

1. RCERESOEUC
2. SEHTLAT
3. OOCUPSENRE
4. GDREAUWIR
5. EHEDISNLT
6. LREÁOTAKRCE
7. RŠKOSCVAÝ
8. CLWHKSIITL

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Slova, která popisují dobrou VPN aplikaci			
2	Situace, kdy pomůže kill switch			
3	Důvody, proč si vybrat Proton VPN			
4	Otázky pro zákaznickou podporu Proton VPN			
5	Věci, které Proton VPN dokáže skrýt před vaší sítí			
6	Lidé, kterým byste doporučili Proton VPN			
7	Zařízení, na která byste nainstalovali Proton VPN			
8	Streamovací služby, které sledujete			
9	Vlastnosti, které hledáte u Proton VPN			
10	Co si ověřit před koupí VPN			
11	Věci, které děláte online každý den			
12	Známky toho, že je vaše VPN připojení pomalé			
13	Země, kde byste chtěli servery Proton VPN			
14	VPN služby jiné než Proton VPN			
15	Místa, kde byste zapnuli Proton VPN			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: OBRANA SECURE CORE



Scénář: Aktivista za lidská práva v restriktivní zemi potřebuje nahrát dokumentaci zahraničnímu tisku. Z obavy, že by místní ISP mohl sledovat výstupní uzel VPN, směruje svůj provoz přes server Secure Core Proton VPN ve Švýcarsku, než provoz pokračuje do cílového uzlu.

Otázka k diskusi: Jak Secure Core brání místním úřadům ve vysledování IP uživatele na výstupním uzlu?

PŘÍPADOVÁ STUDIE 2: OBCHÁZENÍ POMOCÍ PROTOKOLU STEALTH



Scénář: Univerzitní výzkumník cestující do zahraničí zjistí, že jeho studentská kolej blokuje standardní porty OpenVPN (1194) i UDP připojení WireGuard. Aktivuje proto protokol Stealth v klientovi Proton VPN pro Android.

Otázka k diskusi: Jakou technickou metodu používá protokol Stealth k obejití blokací firewallu?

Kontrolní bod 9: Dešifrování šifry

Síťový inženýr zabezpečuje směrovací kanály a klientské tunely. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

28	8	26	35	8	26	38		24	26	22	30	22	20		35	24	20		
35	38	32	41	15	35	1	16	15		17	1	20	2	18	38				
		28	8	4	32	26	8		4	22	26	8							

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky k VPN (část A)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q1: Co je funkce Secure Core od Proton VPN?

Secure Core směruje váš provoz přes více fyzických serverů umístěných ve vysoce bezpečných zemích příznivých pro soukromí (Švýcarsko, Island nebo Švédsko), než vystoupí k cílové destinaci, a chrání tak před korelačními útoky na síť.

Q2: Jak funguje NetShield od Proton VPN?

NetShield je DNS filtr, který blokuje dotazy DNS na známé domény reklam, trackerů a malwaru, brání jejich načtení v prohlížeči a šetří přenosy.

Q3: Jsou aplikace Proton VPN open source?

Ano, všechny aplikace Proton VPN jsou plně open-source a jejich zdrojový kód je zveřejněn na GitHubu spolu s nezávislými profesionálními auditními zprávami.

Q4: Co je Proton VPN Accelerator?

Proton VPN Accelerator je soubor technologií, které využívají řízení zahlcení BBR, více jader procesoru a vyladěný síťový stack ke zvýšení rychlostí připojení až o 400 % na vzdálených serverech.

Q5: V jaké jurisdikci Proton VPN působí?

Proton VPN působí pod jurisdikcí Švýcarska, řídí se přísnými švýcarskými zákony na ochranu soukromí, nezávislými na EU a USA.

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q6: Co je NetShield od Proton VPN?

NetShield je obsahový filtr založený na DNS, který blokuje malware, sledovací skripty a reklamy a šetří mobilní data.

Q7: Podporuje Proton VPN Tor over VPN?

Ano, Proton VPN nabízí dedikované servery, které automaticky směrují veškerý provoz přes anonymizační síť Tor a umožňují přístup k onion webům bez prohlížeče Tor Browser.

Q8: Kolik zařízení mohu připojit k Proton VPN?

Proton VPN podporuje až 10 souběžných připojení zařízení v rámci standardních prémiových plánů. [2]

Q9: Mohu Proton VPN používat k bezpečnému sdílení souborů?

Ano, Proton VPN má dedikované P2P optimalizované servery s vysokorychlostní šířkou pásma, navržené pro bezpečné torrentování.

Q10: Má Proton VPN bezplatnou úroveň?

Ano, Proton VPN nabízí bezplatnou verzi s neomezenou šířkou pásma, ale omezuje přístup na servery v několika zemích a nezahrnuje NetShield ani Secure Core.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část C)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q1: Čím se protokol Stealth liší od standardního OpenVPN?

Na rozdíl od standardního OpenVPN, které používá rozpoznatelné porty a hlavičky, Stealth tuneluje WireGuard přes obfuskované TLS na TCP. Díky tomu vypadá VPN provoz jako běžná HTTPS spojení, což pomáhá vyhnout se blokacím DPI v cenzurovaných zemích.

Q2: Kde jsou fyzicky umístěna serverová zařízení Secure Core?

Servery Secure Core se nacházejí ve Švýcarsku, na bývalé vojenské základně na Islandu a v podzemním datovém centru ve Švédsku, přičemž všechny plně vlastní a provozuje Proton. [1]

Q3: Podporuje Proton VPN ochranu proti únikům IPv6?

Ano, Proton VPN má nativní IPv6 směrování a ochranu proti únikům a automaticky blokuje IPv6 provoz na úrovni systému, pokud jej zabezpečený tunel nepodporuje, aby zabránila odhalení dat.

Q4: Jak NetShield rozlišuje mezi reklamami a malwarovými doménami?

NetShield porovnává odchozí požadavky DNS se známými černými listinami domén. Úroveň 1 blokuje malware, úroveň 2 blokuje malware, sledovací pixely a reklamní sítě.

Q5: Jak VPN Accelerator optimalizuje škálování TCP okna?

Používá algoritmus řízení zahlcení BBR, rozděluje dlouhé trasy na kratší úseky a spouští na serverech Protonu paralelní procesy ke snížení latence a poklesů rychlosti na vzdálených uzlech.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část D)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q6: Jak síť Secure Core odolává fyzické manipulaci se servery?

Proton své servery Secure Core sám dodává, instaluje a provozuje ve vysoce zabezpečených zařízeních a všechny servery Proton VPN používají šifrování celého disku k ochraně svých certifikátů a konfigurace.

Q7: Jaký je kryptografický základ seznamů NetShield od Protonu?

NetShield používá vyhrazené DNS servery Proton, které kontrolují každou doménu proti databázím domén známých hostováním malwaru, reklam nebo trackerů.

Q8: Jak VPN Accelerator optimalizuje využití jader CPU?

Accelerator rozděluje zpracování připojení mezi více jader CPU místo jediného vlákna, čímž snižuje úzká hrdla zpracování na vysokorychlostních serverech.

Q9: Jaký obfuskační mechanismus používá protokol Stealth?

Stealth provozuje WireGuard uvnitř obfuskovaného TLS tunelu přes TCP místo UDP, takže provoz připomíná běžné HTTPS a hloubková inspekce paketů jej hůře odhalí.

Q10: Jak Proton VPN zajišťuje DNS směrování bez úniků na linuxových systémech?

Aplikace pro Linux posílá DNS dotazy tunelem VPN na DNS servery Protonu a její kill switch blokuje provoz, pokud tunel spadne.

Část 11: 10 faktů a poznatků o VPN z praxe

Projděte si fakta z praxe o rychlostech VPN šifrování, auditech protokolů, mobilní konektivitě a podnikové práci na dálku.

1. VPN POSTŘEH

Proton VPN vyvíjí Proton AG, švýcarská společnost založená vědci, kteří se poznali v CERNu v Ženevě. [5]

2. VPN POSTŘEH

Poskytovatel vlastní a provozuje servery Secure Core na vysoce zabezpečených místech ve Švýcarsku, na Islandu (bývalá vojenská základna) a ve Švédsku. [1]

3. VPN POSTŘEH

Zdrojové kódy klientů Proton VPN jsou plně open source a veřejně hostované na GitHubu pro audity třetích stran. [6]

4. VPN POSTŘEH

Technologie NetShield blokuje reklamy, škodlivé skripty a trackery na úrovni DNS dříve, než se dostanou do zařízení uživatele.

5. VPN POSTŘEH

Protokol Stealth tuneluje WireGuard přes obfuskované TLS, aby obešel bloky hloubkové inspekce paketů. [4]

6. VPN POSTŘEH

Proton VPN Accelerator využívá optimalizaci vícejádrového zpracování ke zvýšení rychlostí na vzdálených serverech. [3]

7. POSTŘEH K VPN

Švýcarské právo na ochranu dat obecně vyžaduje švýcarský právní proces, než mohou být předána metadata uživatelů. [5]

8. POSTŘEH K VPN

Vysokorychlostní serverová síť Protonu nabízí připojení až 10 Gbps (k září 2026). [2]

9. POSTŘEH K VPN

Systémový kill switch blokuje veškerý internetový provoz, pokud je aktivní připojení VPN přerušeno.

10. VPN POSTŘEH

Split tunneling funguje na Windows, macOS, Linuxu, Androidu a Android TV a směruje zvolené aplikace mimo VPN. [2]

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních technických standardů, specifikací a regulačních rámců.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (2021). Increase VPN speeds by up to 400% with VPN Accelerator.
https://protonvpn.com/blog/vpn-accelerator

[4] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[5] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

[7] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[8] Cardwell, N., & Cheng, Y. (2017). TCP BBR congestion control comes to GCP – your Internet just got faster.
https://cloud.google.com/blog/products/networking/tcp-bbr-congestion-control-comes-to-gcp-your-internet-just-got-faster

[9] Tor Project. (n.d.). Onion services - Features - Tor Browser.
https://support.torproject.org/onionservices/

[10] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

[11] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká funkce Protonu směruje provoz přes bezpečné země? → Secure Core

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká je hlavní funkce NetShield od Proton VPN? → Blokátor reklam a malwaru na úrovni DNS

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaký protokol Protonu obchází DPI pomocí TLS handshaků? → Protokol Stealth

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je jedinečné na zdrojovém kódu klientů Proton VPN? → Plně open-source a veřejně auditované [6]

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Proton uvádí, že VPN Accelerator kombinuje řízení zahlcení BBR s vícevláknovým zpracováním pro zvýšení rychlosti.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Technologie Secure Core od Proton VPN směruje provoz uživatelů nejprve přes hardwarově zabezpečené fyzické servery umístěné v neutrálních, vysoce zabezpečených jurisdikcích.

7 **Otázka 7** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

NetShield funguje tak, že zachytává a blokuje požadavky na připojení k doménám trackerů a malwaru ve fázi dotazu DNS.

8 **Otázka 8** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: všechny aplikace Proton VPN jsou open source a prošly nezávislými audity.

9 **Otázka 9** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Protokol Stealth balí VPN pakety do standardního šifrování TLS, takže jsou k nerozeznání od HTTPS provozu.

10 **Otázka 10** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Proton VPN sídlí ve Švýcarsku, které je mimo alianci 14 Eyes.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. Secure Core	D 2. NetShield	F 3. Stealth	C 4. Akcelerátor
B 5. Open source	E 6. Švýcarsko	A 7. WireGuard	G 8. Kill Switch

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 STEALTH	2 OPEN SOURCE	3 NETSHIELD	4 SECURE CORE
5 AKCELERÁTOR	6 ŠVÝCARSKO		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – AKCELERÁTOR	2 E – OPENSOURCE	3 G – WIREGUARD	4 F – ŠVÝCARSKO
5 C – STEALTH	6 B – NETSHIELD	7 H – KILLSWITCH	8 A – SECURECORE

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Secure Core, NetShield a Stealth a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

C	D	Ž	V	Ě	K	G	N	Ž	D	Ň	Ď	Ř	X	Q
C	R	Ú	B	A	Ž	O	E	D	L	Š	A	Ď	Ó	Ď
E	A	É	G	I	D	S	T	Ř	N	V	E	I	Š	Ž
C	U	T	É	Ř	Ů	E	S	A	Á	Ý	Ř	P	O	Q
R	G	U	Y	R	A	J	H	S	U	C	Š	Č	K	Ň
U	E	Ý	B	Ě	K	Š	I	X	W	A	Í	A	I	S
O	R	Ž	Ý	Ý	C	L	E	F	I	R	N	S	L	J
S	I	N	M	Ť	E	P	L	G	R	S	Ř	G	L	Ž
N	W	Á	Ó	Ů	L	Ě	D	Ú	C	K	Ý	H	S	Š
E	Ý	B	G	M	E	Ž	F	J	Ó	O	Q	T	W	O
P	S	E	C	U	R	E	C	O	R	E	X	L	I	C
O	N	Ž	Z	Ě	Á	Ý	P	W	Ú	L	Ů	A	T	Q
B	Ó	V	Ť	N	T	F	Ů	Č	Ý	Ú	K	E	C	S
Á	X	Ž	Y	N	O	Š	R	X	H	P	D	T	H	Á
Č	J	Ř	V	W	R	X	L	Í	H	U	H	S	Ě	B

ŘEŠENÍ KŘÍŽOVKY

Š		K	I	L	L	S	W	I	T	C	H
V						E					
Ý			O			C		N		W	
C			P			U		E		I	
A	K	C	E	L	E	R	Á	T	O	R	
R			N			E		S		E	
S			S			C		H		G	
K			O			O		I		U	
O			U			R		E		A	
			R			E		L		R	
			C					D		D	
	S	T	E	A	L	T	H				

PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: KILLSWITCH Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10 písmen)

7 vodorovně: AKCELERÁTOR Optimalizační výkonnostní engine rozdělující zátěž procesoru (11 písmen)

8 vodorovně: STEALTH Vlastní obfuskovaný protokol navržený k obcházení DPI filtrů (7 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ŠVÝCARSKO Ústřední jurisdikce ochrany soukromí se sídlem ve Švýcarsku (9 písmen)

3 svisle: SECURECORE Vícenásobné směrování přes vysoce zabezpečené serverové uzly (10 písmen)

4 svisle: OPENSOURCE Veřejně čitelný repozitář zdrojového kódu aplikace (10 písmen)

5 svisle: NETSHIELD Blokátor reklam, sledovačů a malwaru na úrovni DNS (9 písmen)

6 svisle: WIREGUARD Moderní vysokorychlostní open-source protokol připojení (9 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. RCERESOEUC — **SECURECORE**
2. SEHTLAT — **STEALTH**
3. OOCUPSENRE — **OPENSOURCE**
4. GDREAUWIR — **WIREGUARD**
5. EHEDISNLT — **NETSHIELD**
6. LREÁOTAKRCE — **AKCELERÁTOR**
7. RŠKOSCVAÝ — **ŠVÝCARSKO**
8. CLWHKSIITL — **KILLSWITCH**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"SERVERY PROTON VPN VYUŽÍVAJÍ KANÁLY SECURE CORE"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: OBRANA SECURE CORE

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Aktivista za lidská práva v restriktivní zemi potřebuje nahrát dokumentaci zahraničnímu tiskovému médiu. Z obavy, že by místní ISP mohl monitorovat výstupní uzel VPN, vede provoz nejprve přes server Proton VPN Secure Core ve Švýcarsku a teprve poté k cílovému uzlu.
- Doporučená strategie a řešení: Protože výstupní uzel vidí pouze provoz přicházející ze serveru Secure Core ve Švýcarsku, korelační útok na výstupním serveru nemůže odhalit skutečnou domácí IP aktivisty.

B PŘÍPADOVÁ STUDIE 2: OBCHÁZENÍ POMOCÍ PROTOKOLU STEALTH

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Univerzitní výzkumník na cestách v zahraničí zjistí, že studentská kolej blokuje standardní porty OpenVPN (1194) i UDP spojení WireGuardu. Aktivuje protokol Stealth Proton VPN na svém klientovi pro Android.
- Doporučená strategie a řešení: Stealth spouští WireGuard uvnitř obfuskovaného TLS tunelu přes TCP, takže provoz vypadá pro firewally s hloubkovou inspekcí paketů jako běžné zabezpečené procházení webu.